HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 1.4
ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC 2
CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH 3
1.1 Mục đích 3
1.2 Mô tả ngắn gọn lý thuyết về các công cụ TrueCrypt. 3
1.3 Mô tả cách thức hoặc phương pháp công cụ TrueCrypt áp dụng để mã hóa file hoặc thư mục 3
CHƯƠNG 2. các bước thực hiện 5
2.1 Chuẩn bị môi trường 5
2.1.1 Cài đặt công cụ ảo hóa 5
2.1.2 Cài đặt TrueCrypt trên Windows 5
2.2 Nội dung thử nghiệm 6
2.2.1 Mã hóa file bằng TrueCrypt 6
2.2.2 Mã hóa thư mục bằng TrueCrypt 8
2.2.3 Sao lưu khóa mã hóa 8
2.2.4 Giải mã và khôi phục dữ liệu 9
KẾT LUẬN 11
TÀI LIỆU THAM KHẢO 11

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

- Hiểu được nguyên tắc hoạt động của các kỹ thuật mã hóa.
- Hiểu được cách thức hoạt động của một số công cụ mã hóa dữ liệu
- Biết sử dụng các công cụ mã hóa để đảm bảo an toàn dữ liệu.

1.2 Mô tả ngắn gọn lý thuyết về các công cụ TrueCrypt.

TrueCrypt là một chương trình phần mềm dành cho hệ điều hành windows, nó cho phép người dùng tạo một hoặc nhiều ổ đĩa ảo trên máy tính nhằm giúp người dùng ghi các dữ liệu như video, nhạc, game, chương trình ứng dụng lên đó mà không phải tốn quá nhiều thời gian, công sức cũng như tiền bạc. TrueCrypt tạo nên một vùng ỗ đĩa ảo trong đó bạn có thể lưu, xóa hoặc mở các tập tin khi mà người khác không thể. Đây là biện pháp bảo vệ an toàn cho bạn trong trường hợp ổ đĩa cứng của bạn gặp vấn đề khiến các file dữ liệu trên máy tính có nguy cơ bị mất, hoặc sự tấn công nhằm ăn cắp các tài khoản cá nhân quan trọng của bạn từ các hacker máy tính.

Cơ chế thiết lập và quản lý của TrueCrypt là mã hóa ổ đĩa trên đường đi (on-the-fly encryption). Nghĩa là dữ liệu tự động được mã hóa hoặc giải mã ngay khi được ghi xuống đĩa cứng hoặc ngay khi dữ liệu được nạp lên mà không có bất kỳ sự can thiệp nào của người dùng. Dữ liệu được lưu trữ trên một ổ đĩa đã được mã hóa (encryption volume) không thể đọc được nếu người dùng không cung cấp đúng khóa mã hóa bằng một trong ba hình thức là mật khẩu (password) hoặc tập tin có chứa khóa (keyfile) hoặc khóa mã hóa (encryption key). Toàn bộ dữ liệu trên ổ đĩa mã hóa đều được mã hóa (ví dụ như tên file, tên folder, nội dung của từng file, dung lượng còn trống, siêu dữ

liệu...)

1.3 Mô tả cách thức hoặc phương pháp công cụ TrueCrypt áp dụng để mã hóa file hoặc thư mục

Các tệp có thể được sao chép vào và từ một ổ đĩa TrueCrypt được gắn kết giống như chúng được sao chép vào / từ bất kỳ đĩa thông thường nào (ví dụ: bằng các thao tác kéo và thả đơn giản). Các tệp sẽ tự động được giải mã một cách nhanh chóng (trong bộ nhớ RAM) khi chúng đang được đọc hoặc sao chép từ một ổ đĩa TrueCrypt được mã hóa. Tương tự, các tệp đang được ghi hoặc sao chép vào ổ đĩa TrueCrypt sẽ tự động được mã hóa ngay lập tức (ngay trước khi chúng được ghi vào đĩa) trong RAM. Lưu ý rằng điều này không có nghĩa là toàn bộ tệp sẽ được mã hóa / giải mã phải được lưu trữ trong RAM trước khi nó có thể được mã hóa / giải mã. . TrueCrypt không bao giờ lưu dữ liệu chưa được mã hóa vào ổ đĩa, dữ liệu được mã hóa luôn được lưu trong RAM. Đây là một phương pháp rất an toàn ngăn chặn việc vô tình truy cập vào các tệp của người dùng

Khi gắn ổ đĩa TrueCrypt hoặc khi thực hiện xác thực trước khi khởi động, các bước sau được thực hiện:

- Bước 1: 512 byte đầu tiên của ổ đĩa (tức là header ổ đĩa tiêu chuẩn) được đọc vào RAM, trong đó 64 byte đầu tiên là salt (xem Thông số kỹ thuật định dạng ổ đĩa TrueCrypt).
- Bước2: Các byte 65536–66047 của ổ đĩa được đọc vào RAM. Nếu có một ổ ẩn trong ổ này (hoặc trong phân vùng phía sau phân vùng khởi động), nó đã đọc header của nó tại thời điểm này; nếu không, nó vừa đọc dữ liệu ngẫu nhiên (có hay không một tập đĩa ẩn bên trong nó phải được xác định bằng cách cố gắng giải mã dữ liệu này.
- Bước 3: Bây giờ TrueCrypt cố gắng giải mã header ổ đĩa tiêu chuẩn được đọc trong bước 1. Tất cả dữ liệu được sử dụng và tạo ra trong quá trình giải mã được lưu trong RAM (TrueCrypt không bao giờ lưu chúng vào đĩa). Các thông số sau là không xác định và phải được xác định thông qua quá trình thử và sai (tức là bằng cách thử nghiệm tất cả các kết hợp có thể có của những điều sau):
    - PRF được sử dụng bởi chức năng dẫn xuất khóa header có thể là một trong những chức năng sau: HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool. Mật khẩu do người dùng nhập (mà một hoặc nhiều tập tin khóa có thể đã được áp dụng và salt đọc trong (B1) được chuyển đến hàm dẫn xuất khóa header, hàm này tạo ra một chuỗi giá trị, salt và số lần lặp lại) mà từ đó khóa mã hóa header và khóa header phụ (chế độ XTS) được hình thành. (Các phím này được sử dụng để giải mã header ổ đĩa.)
    - Thuật toán mã hóa: AES-256, Serpent, Twofish, AES-Serpent, ...
    - Phương thức hoạt động: XTS, LRW (không dùng nữa / kế thừa), CBC (không dùng nữa / kế thừa)
- Bước 4: Giải mã được coi là thành công nếu 4 byte đầu tiên của dữ liệu được giải mã chứa chuỗi ASCII “TRUE” và nếu tổng kiểm tra CRC-32 của 256 byte cuối cùng của dữ liệu được giải mã (header tập) khớp với giá trị nằm ở byte # 8 của dữ liệu được giải mã. Nếu các điều kiện này không được đáp ứng, quá trình lại tiếp tục từ (B3), nhưng lần này, thay vì dữ liệu được đọc trong (B1), dữ liệu được đọc trong (B2) được sử dụng (tức là có thể có header tập đĩa ẩn). Nếu các điều kiện không được đáp ứng một lần nữa, quá trình gắn kết sẽ bị chấm dứt (sai mật khẩu, ổ đĩa bị hỏng hoặc không phải là ổ đĩa TrueCrypt).
- Bước 5: Bây giờ chúng ta biết (hoặc giả sử với xác suất rất cao) rằng chúng ta có mật khẩu chính xác, thuật toán mã hóa chính xác, chế độ, kích thước khóa và thuật toán dẫn xuất khóa header chính xác. Nếu chúng giải mã thành công dữ liệu được đọc trong (B2), chúng cũng biết rằng chúng tôi đang gắn một tập đĩa ẩn và kích thước của nó được truy xuất từ dữ liệu đọc trong (B2) được giải mã trong (B3).
- Bước 6: Quy trình mã hóa được khởi động lại bằng khóa chính ** và khóa chính phụ, được truy xuất từ header ổ đĩa được giải. Các khóa này có thể được sử dụng để giải mã bất kỳ khu vực nào của ổ đĩa, ngoại trừ vùng header ổ đĩa (hoặc vùng dữ liệu khóa, để mã hóa hệ thống), đã được mã hóa bằng các khóa header. Ổ đĩa được gắn kết.

CHƯƠNG 2. CÁC BƯỚC THỰC HIỆN

2.1 Chuẩn bị môi trường

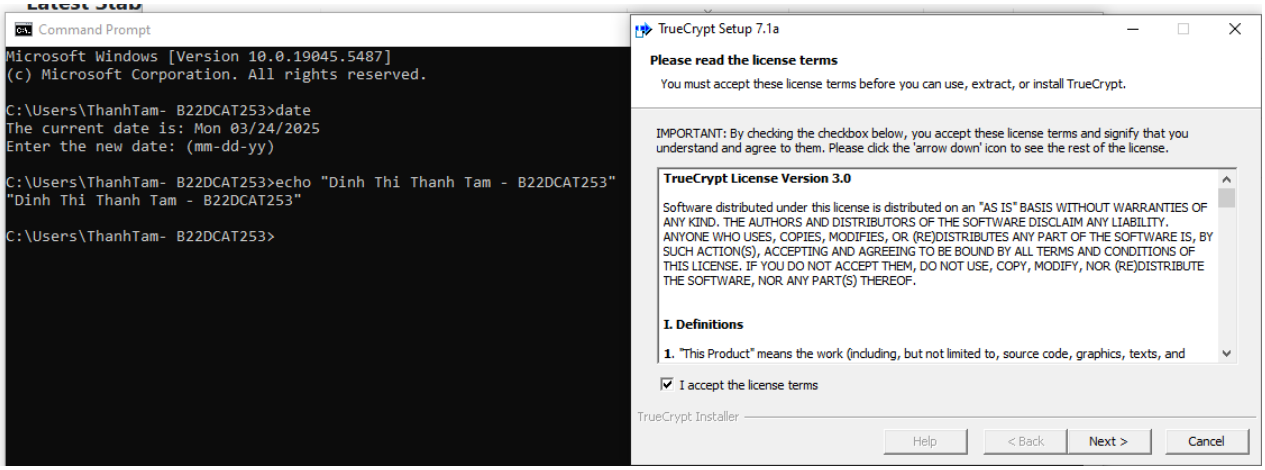
2.1.1 Cài đặt công cụ ảo hóa

- Bước 1: Tải và cài đặt VMware Workstation hoặc VirtualBox.
- Bước 2: Tạo một máy ảo mới, chọn hệ điều hành Windows.
- Bước 3: Cấu hình tài nguyên cho máy ảo (RAM, CPU, dung lượng ổ cứng).
- Bước 4: Cài đặt Windows trên máy ảo.

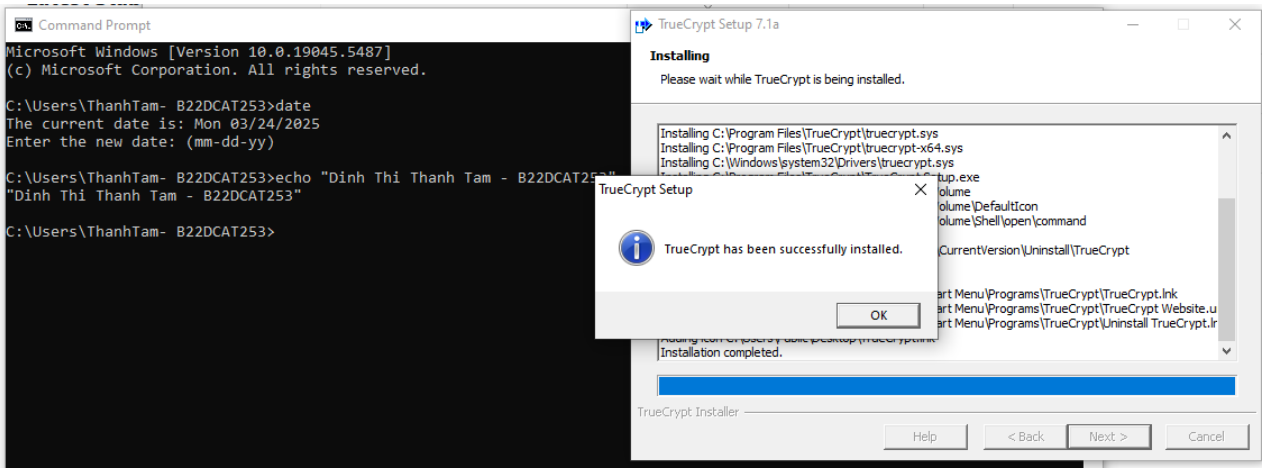
2.1.2 Cài đặt TrueCrypt trên Windows

- Bước 1: Tải phần mềm TrueCrypt từ một nguồn uy tín.

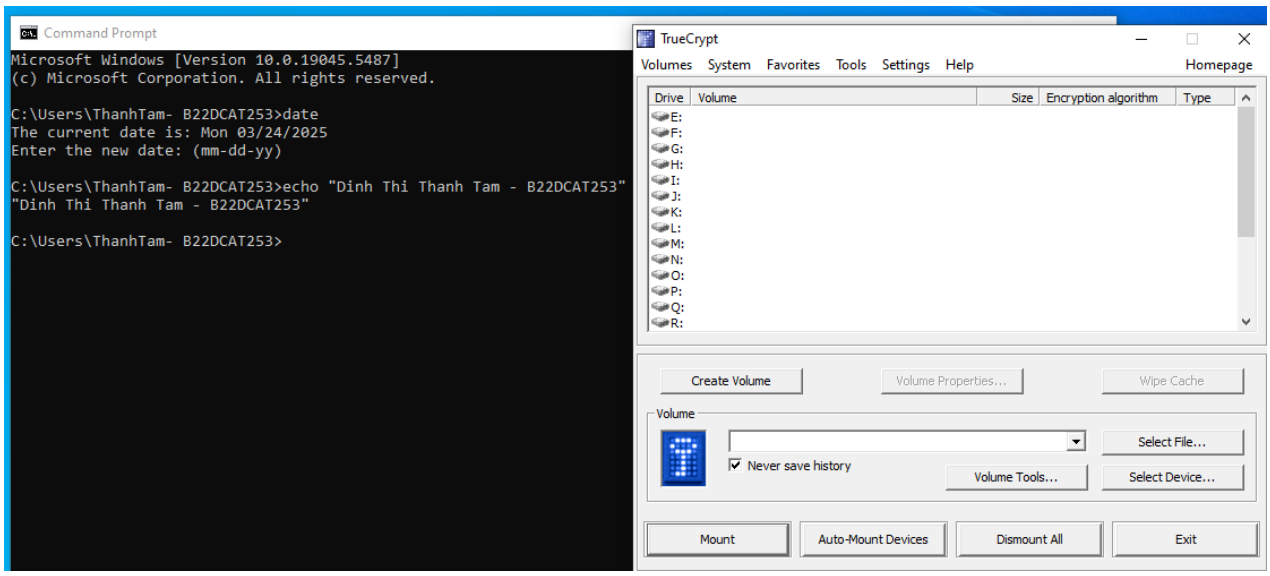
  Tải TrueCrypt từ trang: https://truecrypt.ch/



- Bước 2: Chạy tệp cài đặt, làm theo hướng dẫn để cài đặt TrueCrypt.



- Bước 3: Mở TrueCrypt và kiểm tra xem đã cài đặt thành công chưa.

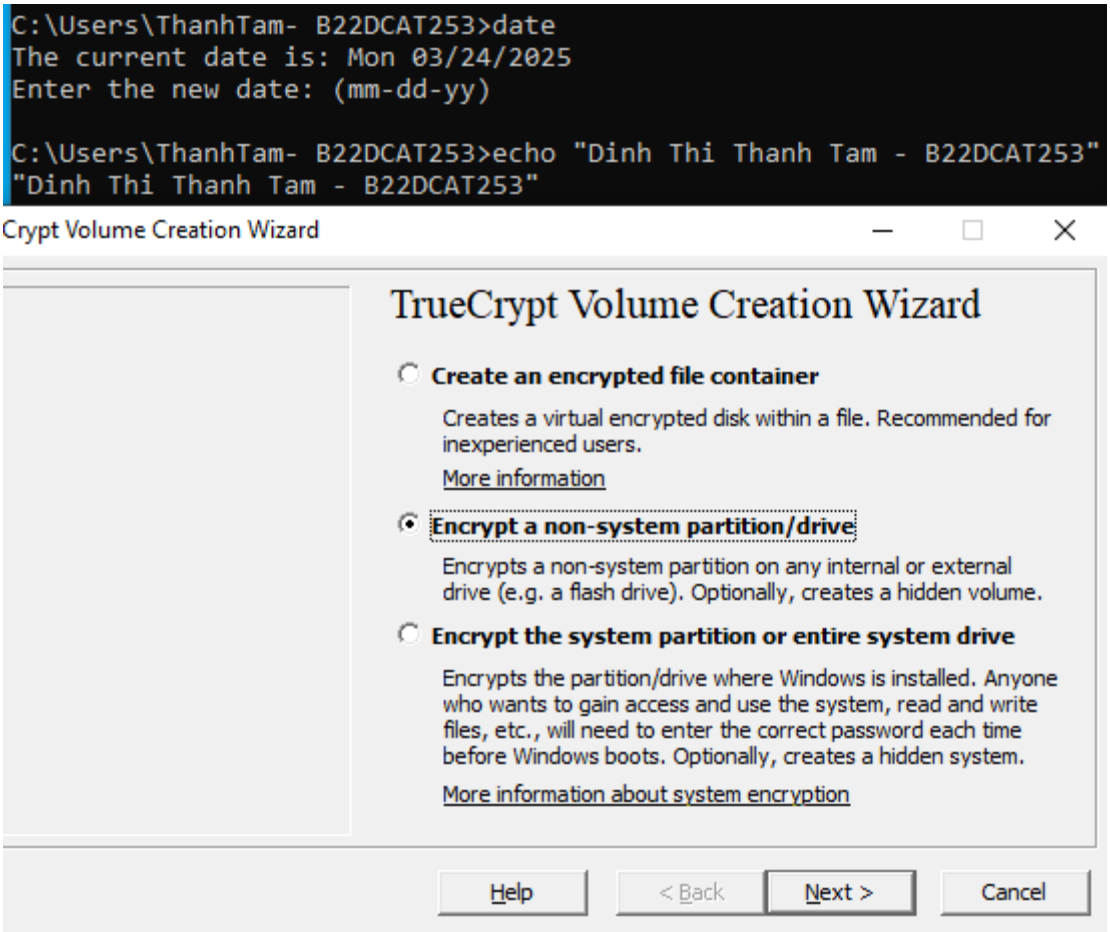


2.2 Nội dung thử nghiệm

2.2.1 Mã hóa file bằng TrueCrypt

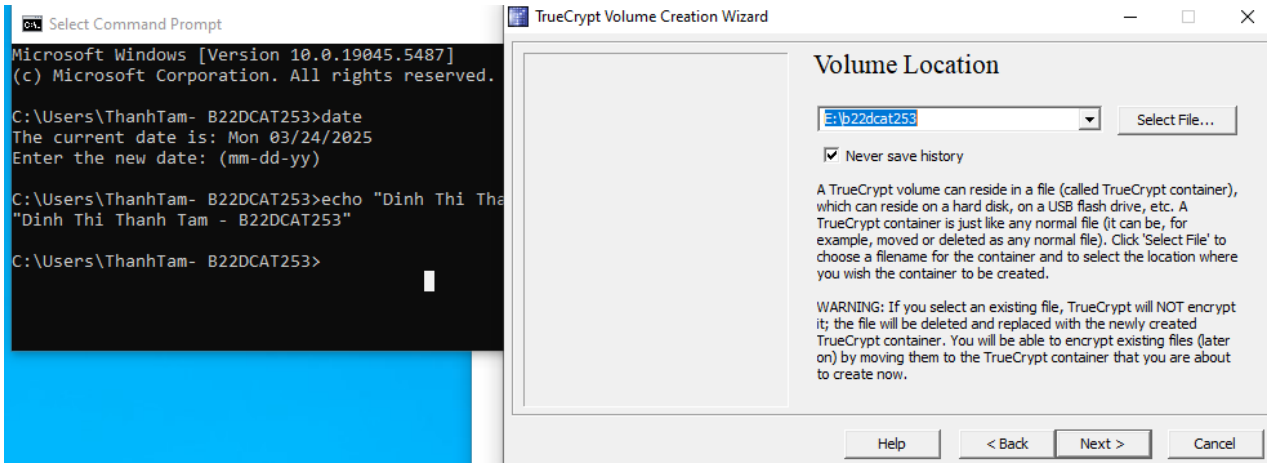
Bước 1: Mở TrueCrypt.

Bước 2: Chọn Create Volume → Chọn Create an encrypted file container (Tạo file mã hóa).



Bước 3: Chọn vị trí lưu file mã hóa, đặt tên file

Lưu tại địa chỉ E:\b22dcat253

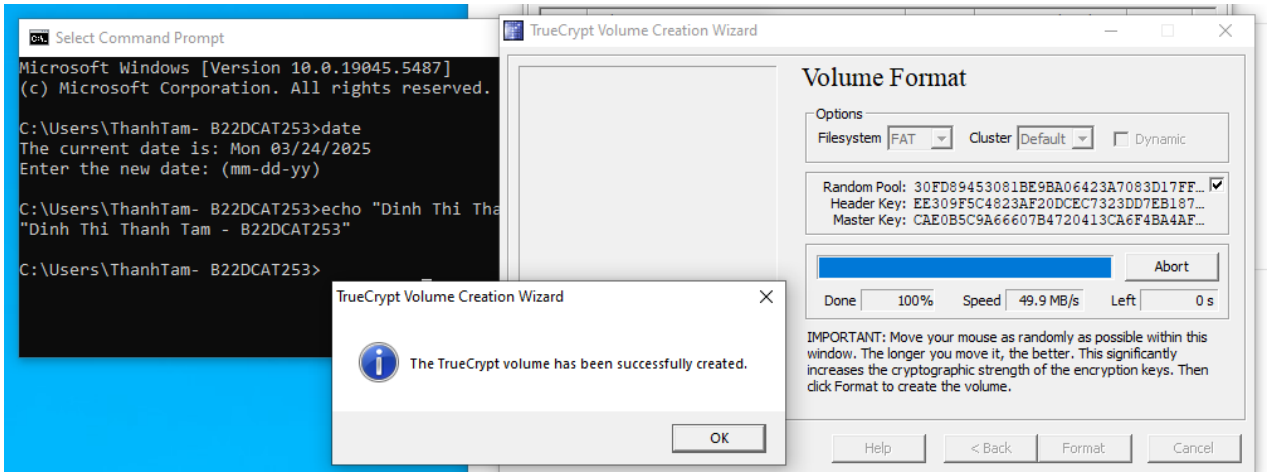


Bước 4: Chọn thuật toán mã hóa và hoàn tất quá trình mã hóa.

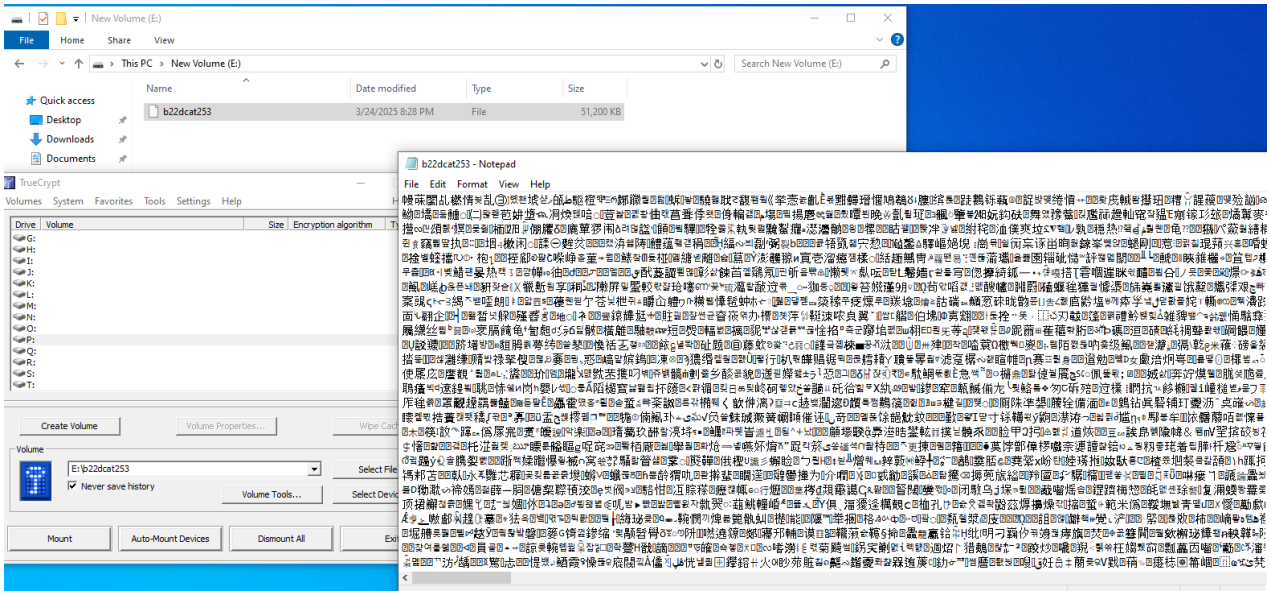
Chọn thuật toán AES

Bước 5: Nhập mật khẩu.

Bước 6: Format ổ mã hóa với định dạng FAT.

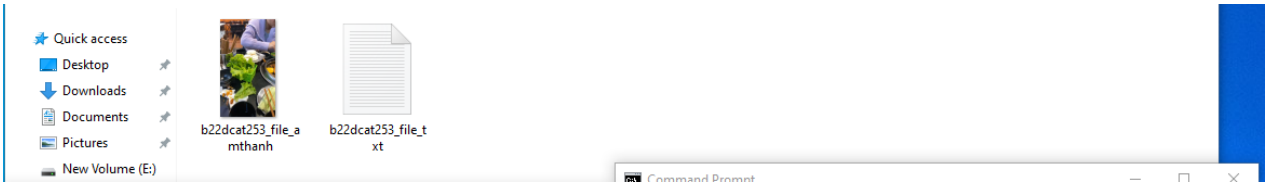


Bước 7: Nhấn Mount, nhập mật khẩu để truy cập vào ổ mã hóa này.



Bước 8: Sao chép file văn bản hoặc file đa phương tiện vào ổ mã hóa.

Thêm file âm thanh b22dcat253_file_amthanh và file văn bản b22dcat253_file_txt vào ổ mã hóa



Chú ý: Thực hiện trên ít nhất 2 loại file: file văn bản (.txt, .docx) và file đa phương tiện (.jpg, .mp4, .mp3).

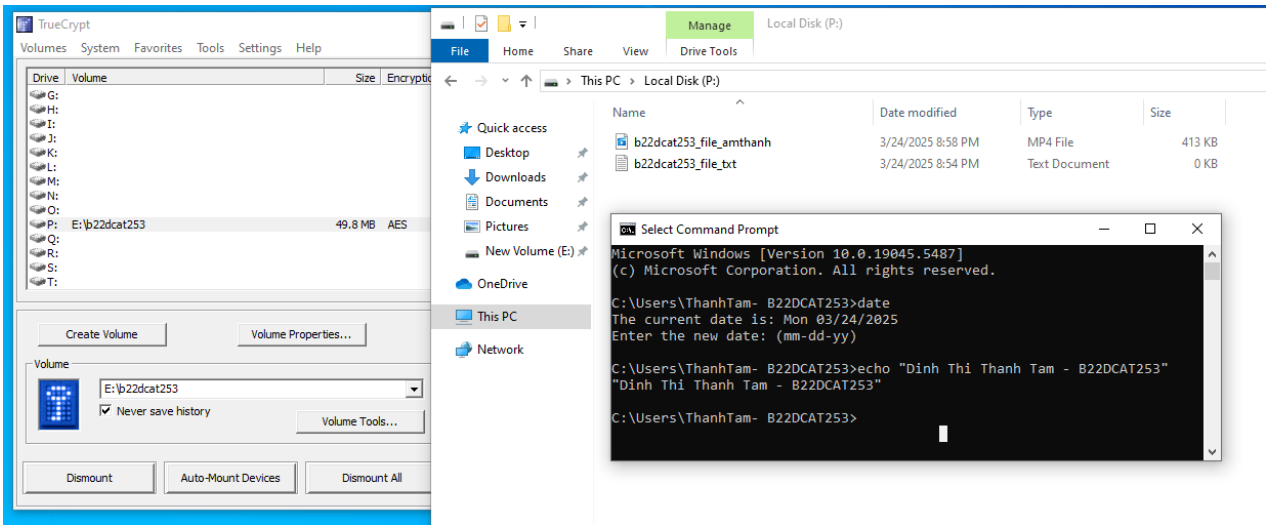
2.2.2 Mã hóa thư mục bằng TrueCrypt

Bước 1: Gắn ổ mã hóa vào hệ thống

- Chọn một ký tự ổ đĩa để lưu file mã hóa, ở đây chọn ổ P
- Nhấn Select File… để chọn thư mục đã tạo b22dcat253 chứa 2 file âm thanh và văn bản
- Nhấn Mount và nhập mật khẩu để mở ổ.

Bước 2: Di chuyển thư mục vào ổ mã hóa

- Sao chép thư mục cần mã hóa (tên thư mục theo mã sinh viên) vào ổ đĩa mã hóa vừa gắn.



Bước 3: Ngắt kết nối ổ mã hóa

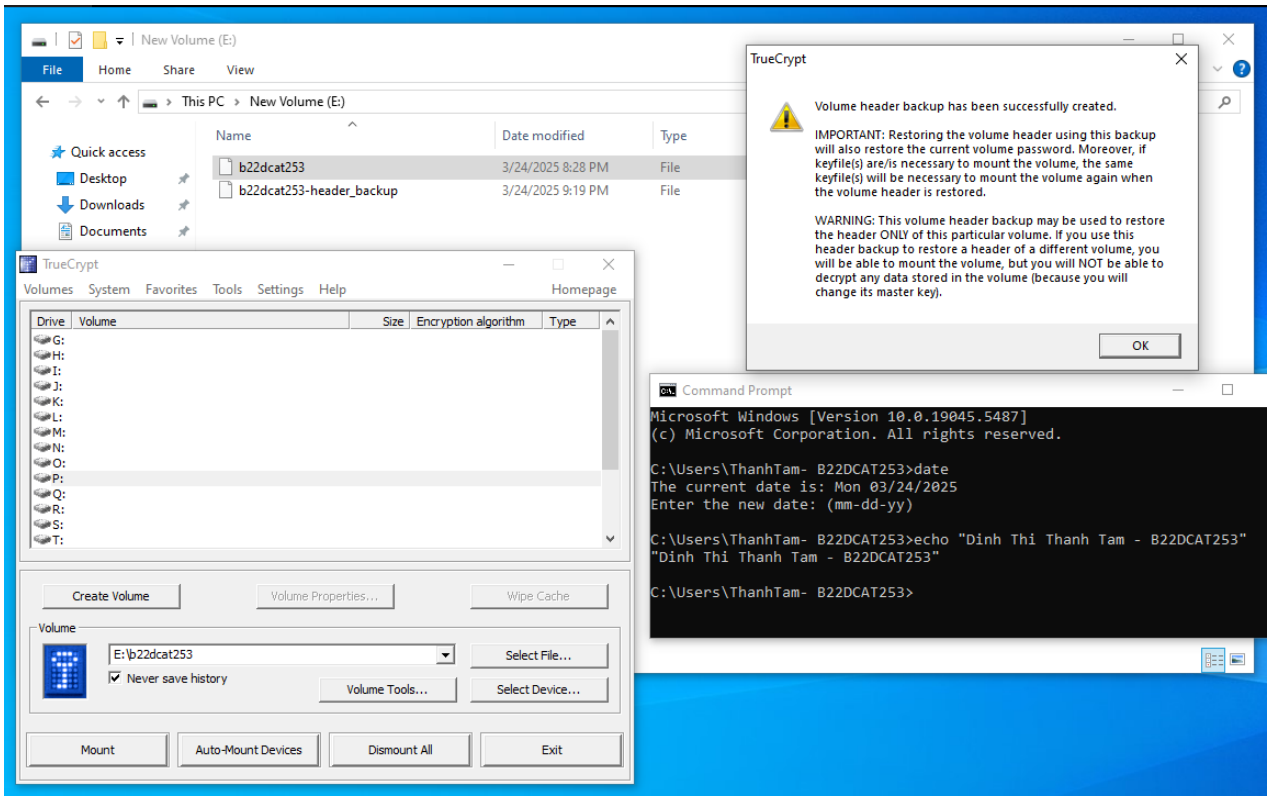
- Quay lại TrueCrypt.
- Chọn ổ đĩa đang gắn (ổ P:)
- Nhấn Dismount để ngắt kết nối.

2.2.3 Sao lưu khóa mã hóa

Bước 1: Trong TrueCrypt, vào Tools → Backup Volume Header.

Bước 2: Lưu file backup ở nơi an toàn.

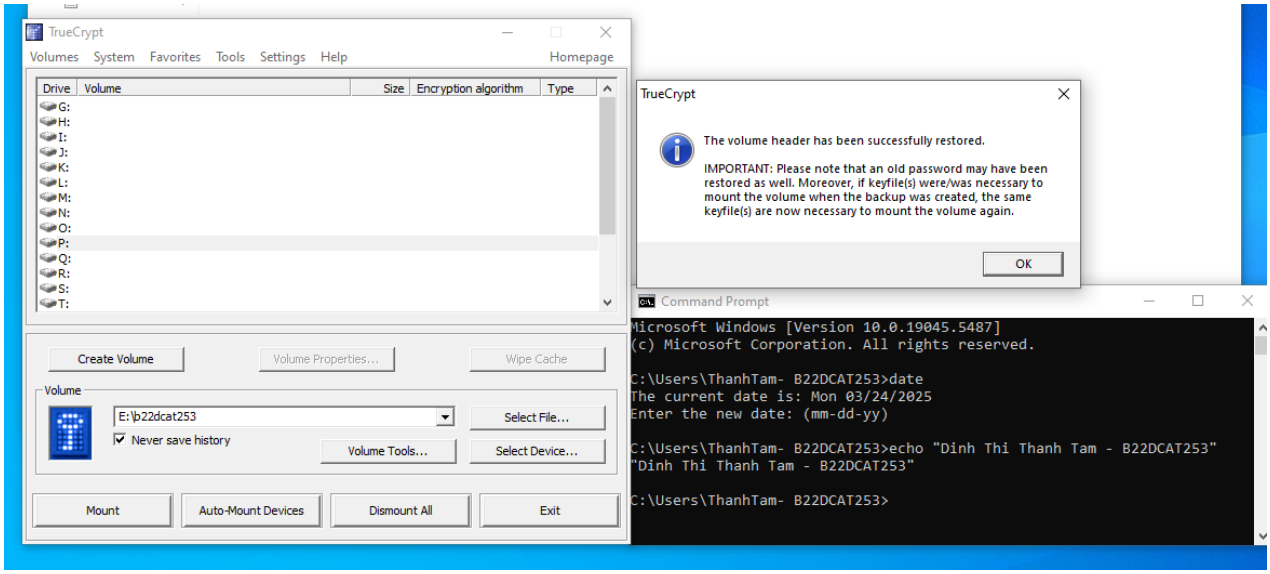
Lưu trong ổ E chứa thư mục b22dcat253 tạo ban đầu



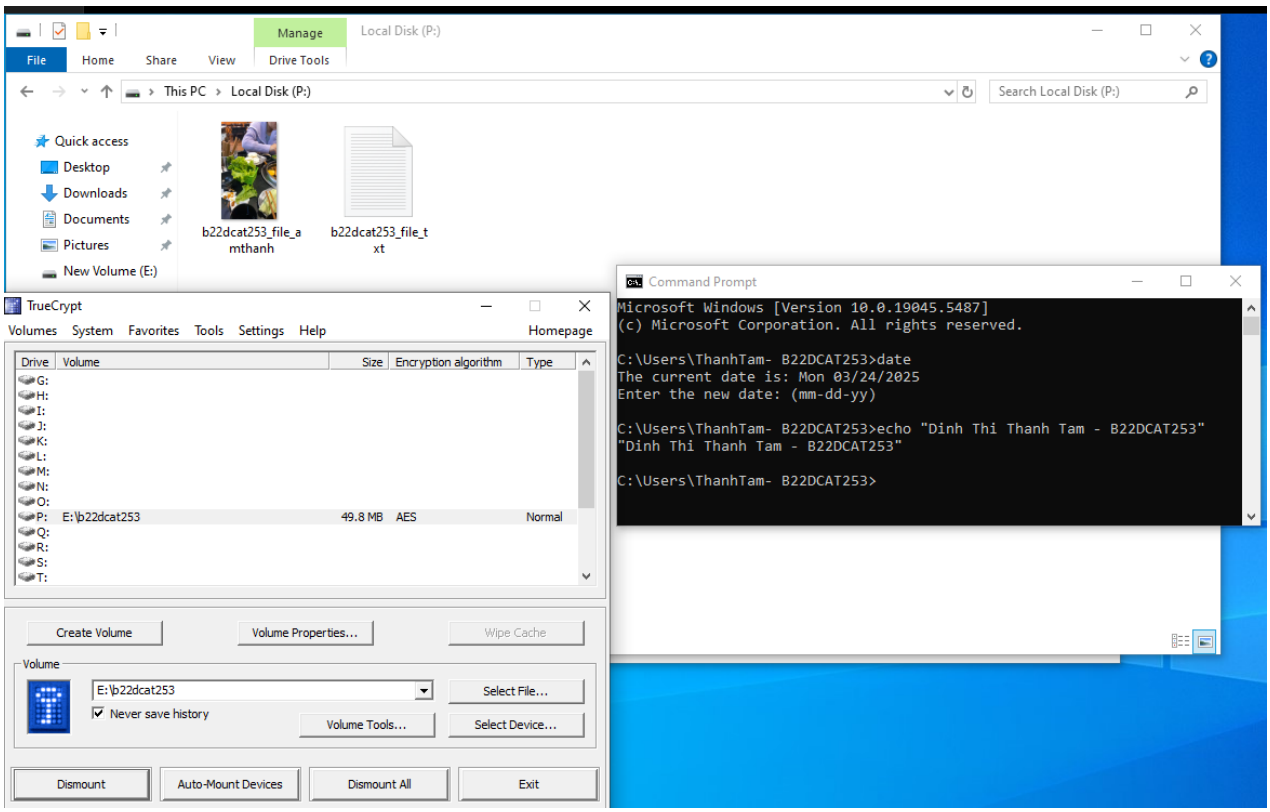
2.2.4 Giải mã và khôi phục dữ liệu

Bước 1: Mở TrueCrypt.

Bước 2: Chọn Mount Volume, nhập mật khẩu để giải mã.



Bước 3: Kiểm tra file/thư mục sau khi giải mã.



⇨ *Đã khôi phục thành công dữ liệu mã hóa*

Bước 4: Chọn Dismount để ngắt kết nối.

KẾT LUẬN

Bài thực hành đã giúp hiểu rõ nguyên tắc hoạt động của mã hóa dữ liệu và cách sử dụng công cụ TrueCrypt để đảm bảo an toàn thông tin. Qua các bước thực hiện, chúng ta đã biết cách tạo, mã hóa và bảo vệ file/thư mục bằng mật khẩu, cũng như cách giải mã và khôi phục dữ liệu khi cần thiết. Việc áp dụng công nghệ mã hóa không chỉ giúp bảo vệ thông tin cá nhân mà còn đóng vai trò quan trọng trong bảo mật dữ liệu doanh nghiệp và tổ chức.

TÀI LIỆU THAM KHẢO

[1] Đỗ Xuân Chợ, Bài giảng Mật mã học cơ sở, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.

[2] Đỗ Xuân Chợ, Bài giảng Mật mã học nâng cao, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.